

Central Intelligence Agency



Washington, D.C. 20505

GAO/Rep

OCA 88-3432

14 OCT 1988

Mr. Howard Rhile
Associate Director
Information Management
and Technology Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Rhile:

The Director has asked me to respond to your 3 October 1988 letter requesting completion of a questionnaire intended to determine federal agencies compliance with sections 5(a) and 5(b) of the Computer Security Act of 1987, Public Law 100-235, 8 January 1988.

After a thorough review of the various computer systems at the Central Intelligence Agency, we have determined that none of our systems are subject to the reporting requirements of the Act. This decision was based on 44 U.S.C. Section 3502(2).

Sincerely,



John L. Helgerson
Director of Congressional Affairs

ORIG: DD/OCA/HA [redacted] (13 October 1988)

Distribution:

Original - Addressee
1 - D/OIT
1 - ER
1 - DDA
1 - D/OS
1 - D/OCA
1 - OGC
1 - OCA Record
1 - NHG/OCA Chrono
1 - OCA Reader



United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

WILLIAM H. WEBSTER
CENTRAL INTELLIGENCE AGENCY

OCT 3 1988

WASHINGTON, DC 20505

The United States General Accounting Office (GAO), part of the legislative branch, assists the Congress in oversight of the executive branch of the federal government. GAO's major responsibilities include evaluating and auditing programs, activities, and financial operations of federal departments and agencies and making recommendations for improving government operations. The Chairmen of the House Committees on Government Operations and Science, Space, and Technology, respectively, asked us to ascertain the extent to which federal agencies are complying with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. (Job code 510306.)

To obtain information on the status of compliance, we are sending three questionnaires to federal agencies. The first, which you have already received, addressed section 6(a) of the act and was directed at the identification of federal computer systems that contain sensitive information.

The second questionnaire, which is enclosed, addresses section 5 of the act. Section 5(a) requires federal agencies to provide training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system containing sensitive information that is within or under the supervision of that agency. Section 5(b) requires such training to be started within 60 days of the issuance of training regulations by the Office of Personnel Management (OPM). OPM issued these regulations on July 13, 1988. One additional questionnaire, to follow in January 1989, will address section 6(b) of the act, which is aimed at the establishment of computer security plans for the security and privacy of federal computer systems that contain sensitive information.

The enclosed questionnaire is being sent to you as the senior information resource management (or comparable) official in your agency. Please complete and return the questionnaire in the enclosed envelope within 10 days of receipt. Please be sure to include in your response information for all offices, bureaus, services, etc. within your agency. If you have any questions, please call Michael Jarvis or David Gill at (202) 275-9675.

Thank you for your cooperation.

Sincerely yours,

Howard Rhile

Howard Rhile
Associate Director

**U.S. General Accounting Office
COMPUTER SECURITY ACT OF 1987 QUESTIONNAIRE**

The U.S. General Accounting Office (GAO) has been asked by the Chairmen of the House Committees on Government Operations and Science, Space, and Technology to review federal agencies' compliance with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. In response, we are sending questionnaires to federal agencies in order to ascertain the extent to which they are in compliance.

The previous questionnaire, which you have already received, addressed section 6(a) of the act and was used to obtain information on the status of federal agencies' identification of federal computer systems that contain sensitive information.

This questionnaire is being used to obtain information from federal agencies on the status of their compliance with section 5 of the act, **FEDERAL COMPUTER SYSTEM SECURITY TRAINING**. Section 5(a) requires federal agencies to provide training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system containing sensitive information that is within or under the supervision of that agency. Section 5(b) requires such training to be started within 60 days after the issuance of the Office of Personnel Management (OPM) regulations prescribing the procedures and scope of training to be provided federal civilian employees and the manner in which such training is to be carried out. OPM issued these regulations on July 13, 1988. According to the act, such training is to be designed to:

- enhance employees' awareness of the threats to and vulnerability of computer systems; and
- encourage the use of improved computer security practices.

Please return the completed questionnaire in the enclosed self-addressed envelope within 10 days of receiving it. If the return envelope has been lost, please send the completed questionnaire to Loraine Przybylski, U.S. General Accounting Office, Room 6075, 441 G St., N.W., Washington, D.C. 20548. If you have any questions, please call Michael Jarvis or David Gill at (202) 275-9675. Thank you for your help.

1. Agency name _____

2. Agency address _____

3. Responsible official to contact for additional information, if needed.

Name _____

Department/Office _____

Address _____

Telephone number _____

4. Does your agency have federal computer systems that contain sensitive information, including systems under development, which are within or under the supervision of your agency? Consider only systems that belong to your agency regardless of whether you or someone else operates the system. Exclude systems that you operate for another agency.

(CHECK ONE)

☐ YES

☐ NO (GO TO QUESTION 13)

5. Section 5(a) of the Computer Security Act of 1987 requires periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system containing sensitive information that is within or under the supervision of that agency. Section 5(b) requires this training to be started within 60 days of the issuance of training regulations by the Office of Personnel Management (OPM), which were issued on July 13, 1988.

Does your agency have a computer system security training program in accordance with this requirement?

(CHECK ONE)

☐ YES
☐ NO

If yes, when was the training program started?

month/day/year

If no, when do you plan to start such a training program?

month/year (GO TO QUESTION 13)

6. Section 5(a) requires mandatory periodic computer security training in accordance with (1) National Bureau of Standards (now National Institute of Standards and Technology) guidelines and OPM regulations or (2) an approved alternative program. If your agency has started a computer security program, indicate how the program meets the act's requirement:

(CHECK ONE)

☐ Follows National Institute of Standards and Technology (NIST) guidelines and OPM regulations
☐ Is an alternative program that has been approved by the agency head and determined to be at least as effective in accomplishing the training objectives of NIST guidelines and OPM regulations

7. For each classroom activity offered in computer security by all offices, bureaus, services, etc. within your agency, please provide the following.

A. Name of course or course module _____

B. Primary subject matters covered by the course include

(Check all that apply)

- ☐ computer security basics (e.g. threats to and vulnerabilities of systems, use of improved security practices, agency-specific policies and procedures)
- ☐ security planning and management
- ☐ computer security policies, procedures, and practices
- ☐ contingency planning
- ☐ security aspects of systems life cycle management
- ☐ other (specify) _____

C. Course was first offered on _____
month/year

D. Purpose of the course is to

(Check all that apply)

- ☐ enhance employees' awareness of the threats to and vulnerability of computer systems
- ☐ encourage use of improved computer security practices

E. Targeted audience includes

(Check all that apply)

- ☐ senior managers
- ☐ functional or program managers
- ☐ security managers
- ☐ auditors
- ☐ end user personnel
- ☐ system development personnel (e.g. designers, analysts, programmers)
- ☐ system maintenance personnel (e.g. analysts, programmers, computer operators)
- ☐ other (specify) _____

F. Course is provided by

- ☐ in-house personnel
- ☐ OPM
- ☐ contractor
- ☐ other (specify) _____

G. Course is offered

- ☐ monthly
- ☐ semiannually
- ☐ annually
- ☐ other (specify) _____

H. Refresher sessions are

- ☐ offered
- ☐ not offered

If offered, refresher sessions are offered

- ☐ monthly
- ☐ semiannually
- ☐ annually
- ☐ other (specify) _____

I. Course is

- ☐ mandatory
- ☐ voluntary

J. Projected date for completion of course for all of target audience is _____
(month/year)

For each activity offered in computer security by all offices, bureaus, services, etc. within your agency (other than classroom training), please provide the following.

K. Type of training includes

(Check all that apply)

- ☐ on-the-job training
- ☐ agency newsletters
- ☐ agency memorandums
- ☐ video tapes
- ☐ pamphlets/brochures
- ☐ posters
- ☐ other (specify) _____

L. Primary subject matters covered by the activity include

(Check all that apply)

- ☐ computer security basics (e.g. threats to and vulnerabilities of systems, use of improved security practices, agency-specific policies and procedures)
- ☐ security planning and management
- ☐ computer security policies, procedures, and practices
- ☐ contingency planning
- ☐ security aspects of systems life cycle management
- ☐ other (specify) _____

M. Activity was first offered on _____
(month/year)

N. Purpose of the activity is to

(Check all that apply)

- ☐ enhance employees' awareness of the threats to and
vulnerability of computer systems
☐ encourage use of improved computer security practices

O. Targeted audience includes

(Check all that apply)

- ☐ senior managers
☐ functional or program managers
☐ security managers
☐ auditors
☐ end user personnel
☐ system development personnel (e.g. designers,
analysts, programmers)
☐ system maintenance personnel (e.g. analysts,
programmers, computer operators)
☐ other (specify) _____

P. Activity is provided by

- ☐ in-house personnel
☐ OPM
☐ contractor
☐ other (specify) _____

Q. Activity is offered

- ☐ monthly
☐ semiannually
☐ annually
☐ other (specify) _____

R. Activity is

- ☐ mandatory
☐ voluntary

S. Projected date for completion of activity for all of targeted
audience is (if applicable) _____
(month/year)

8. Does the information provided in question 7 include all offices, bureaus, services, etc., within your agency?

(CHECK ONE)

☐ YES
☐ NO

If no, what offices, bureaus, services, etc., does it exclude?

9. In preparing your training program, how satisfied was your agency with the content of the July 8, 1988, NIST Draft Computer Security Training Guidelines?

(CHECK ONE)

☐ very satisfied
☐ satisfied
☐ neither satisfied nor dissatisfied
☐ dissatisfied
☐ very dissatisfied
☐ did not use NIST's draft training guidance

10. Were the NIST guidelines helpful in developing your computer security training program?

(CHECK ONE)

☐ YES
☐ NO
☐ NO OPINION

Please provide any comments on NIST's draft training guidance in the space below.

11. In preparing your training program, how satisfied was your agency with the content of OPM's July 13, 1988, Interim Regulation?

(CHECK ONE)

- ☐ very satisfied
- ☐ satisfied
- ☐ neither satisfied nor dissatisfied
- ☐ dissatisfied
- ☐ very dissatisfied
- ☐ did not use OPM's interim training regulation

12. Was the OPM regulation helpful in developing your computer security training program?

(CHECK ONE)

- ☐ YES
- ☐ NO
- ☐ NO OPINION

Please provide any comments on OPM's interim training regulation in the space below.

13. If you have any comments about any of the questions on this form, or if you have any comments about questions you believe we should have asked but did not, please write them below.

Thank you for your cooperation